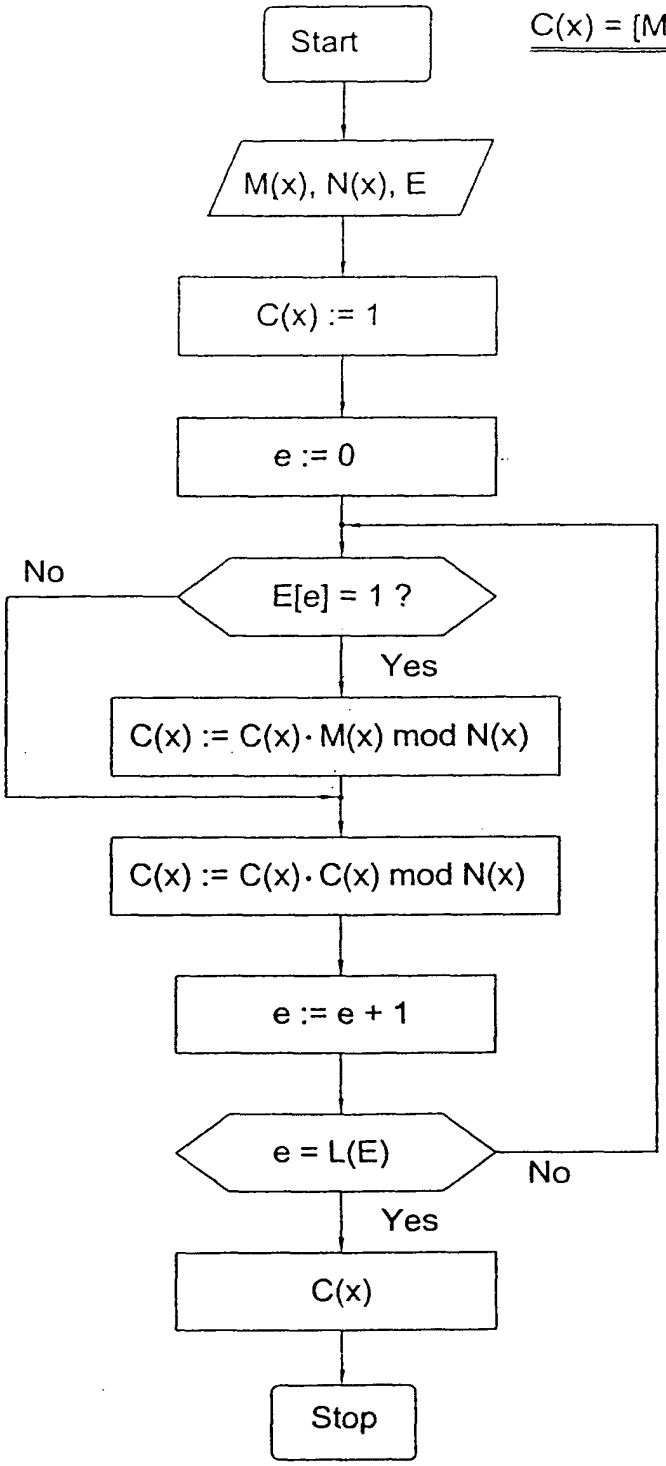

C(x) = [M(x)]^E mod N(x)
Start
M(x), N(x), E
C(x) := 1
e := 0
No
E[e] = 1 ?
Yes
C(x) := C(x) · M(x) mod N(x)
C(x) := C(x) · C(x) mod N(x)
e := e + 1
e = L(E)
No
Yes
C(x)
Stop

FIG 1

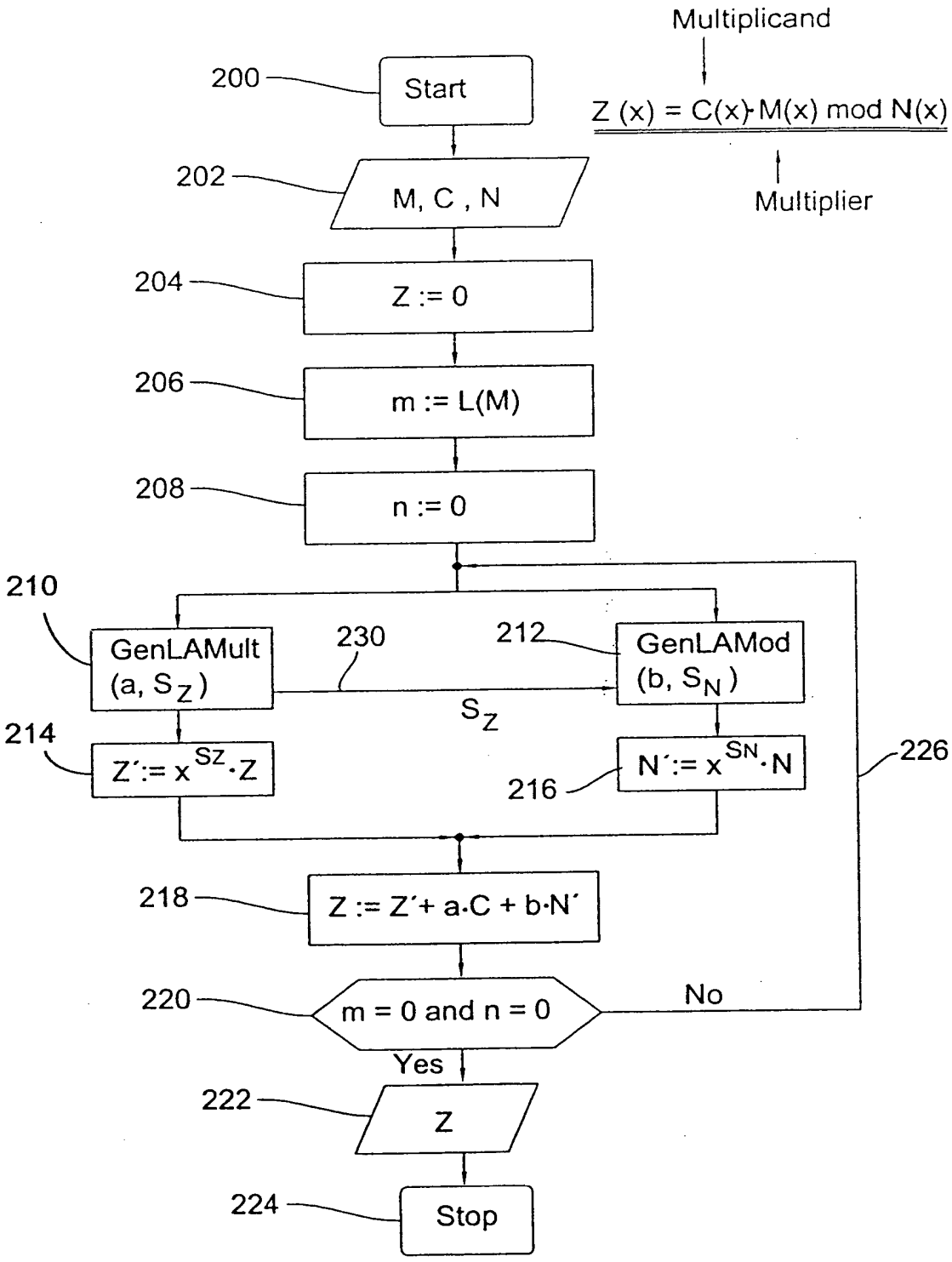

Multiplicand
Z (x) = C(x)·M(x) mod N(x)
Multiplier
200
Start
202
M, C , N
204
Z := 0
206
m := L(M)
208
n := 0
210
GenLAMult
(a, S_Z)
230
S_Z
212
GenLAMod
(b, S_N)
214
Z´:= x^SZ·Z
216
N´:= x^SN·N
226
218
Z := Z´+ a·C + b·N´
220
m = 0 and n = 0
No
Yes
222
Z
224
Stop

FIG 2

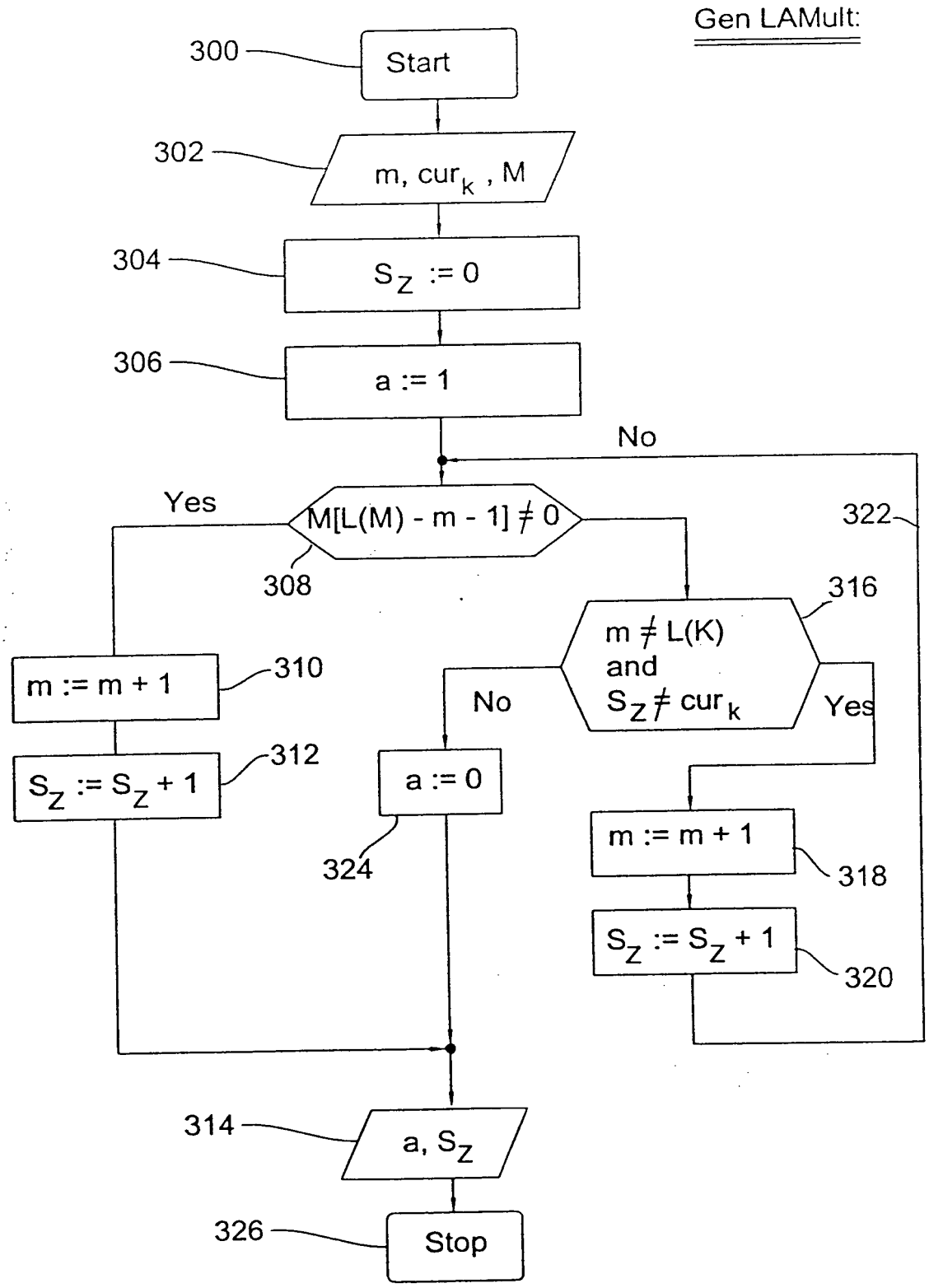

Gen LAMult:
300
Start
302
m, cur$_k$, M
304
S_Z := 0
306
a := 1
No
Yes
M[L(M) - m - 1] ≠ 0
308
322
316
m ≠ L(K)
and
S_Z ≠ cur$_k$
No
Yes
m := m + 1
310
S_Z := S_Z + 1
312
a := 0
324
m := m + 1
318
S_Z := S_Z + 1
320
314
a, S_Z
326
Stop

FIG 3

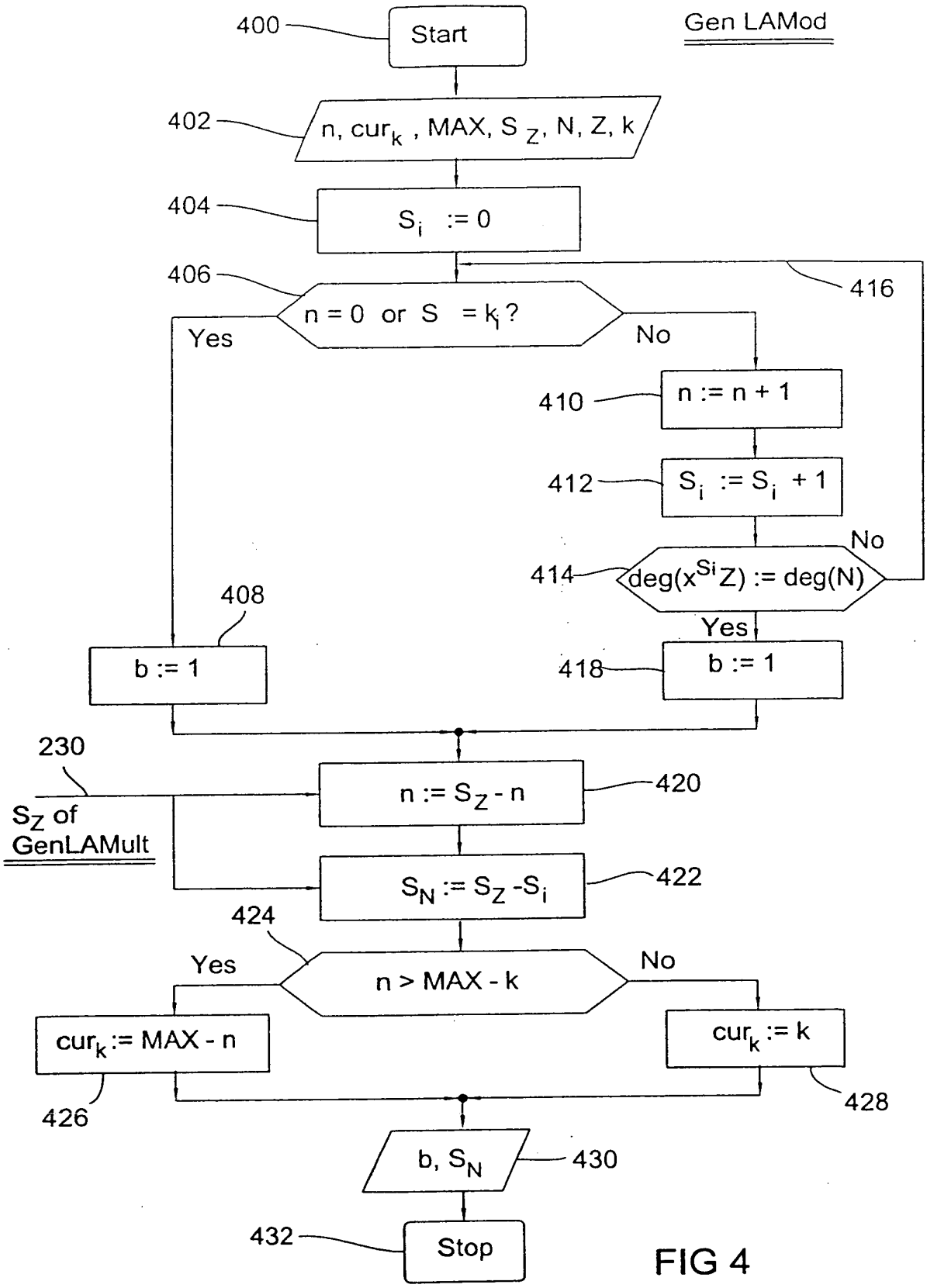

Gen LAMod
400
Start
402
n, cur_k , MAX, S_Z, N, Z, k
404
S_i := 0
406
n = 0 or S = k_i ?
Yes
No
416
410
n := n + 1
412
S_i := S_i + 1
414
deg(x^Si Z) := deg(N)
No
Yes
408
b := 1
418
b := 1
230
S_Z of GenLAMult
420
n := S_Z - n
422
S_N := S_Z - S_i
424
n > MAX - k
Yes
No
cur_k := MAX - n
cur_k := k
426
428
b, S_N
430
432
Stop

FIG 4

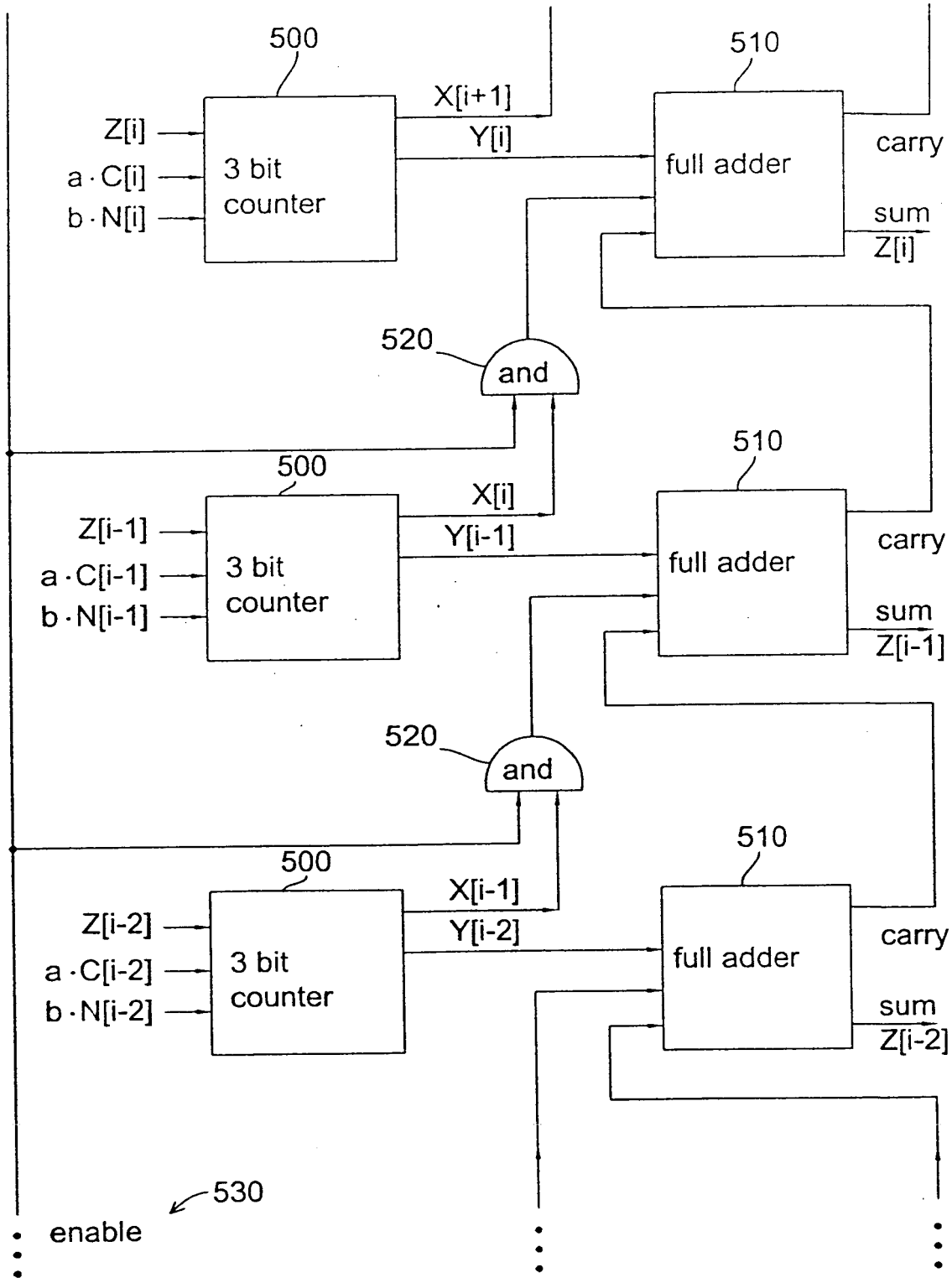
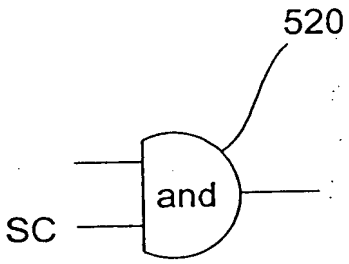

500
510
X[i+1]
Y[i]
Z[i]
a · C[i]
b · N[i]
3 bit counter
full adder
carry
sum Z[i]
520
and
500
510
X[i]
Y[i-1]
Z[i-1]
a · C[i-1]
b · N[i-1]
3 bit counter
full adder
carry
sum Z[i-1]
520
and
500
510
X[i-1]
Y[i-2]
Z[i-2]
a · C[i-2]
b · N[i-2]
3 bit counter
full adder
carry
sum Z[i-2]
530
enable

FIG 5



SC = 1 for normal addition
SC = 0 for XOR

FIG 6

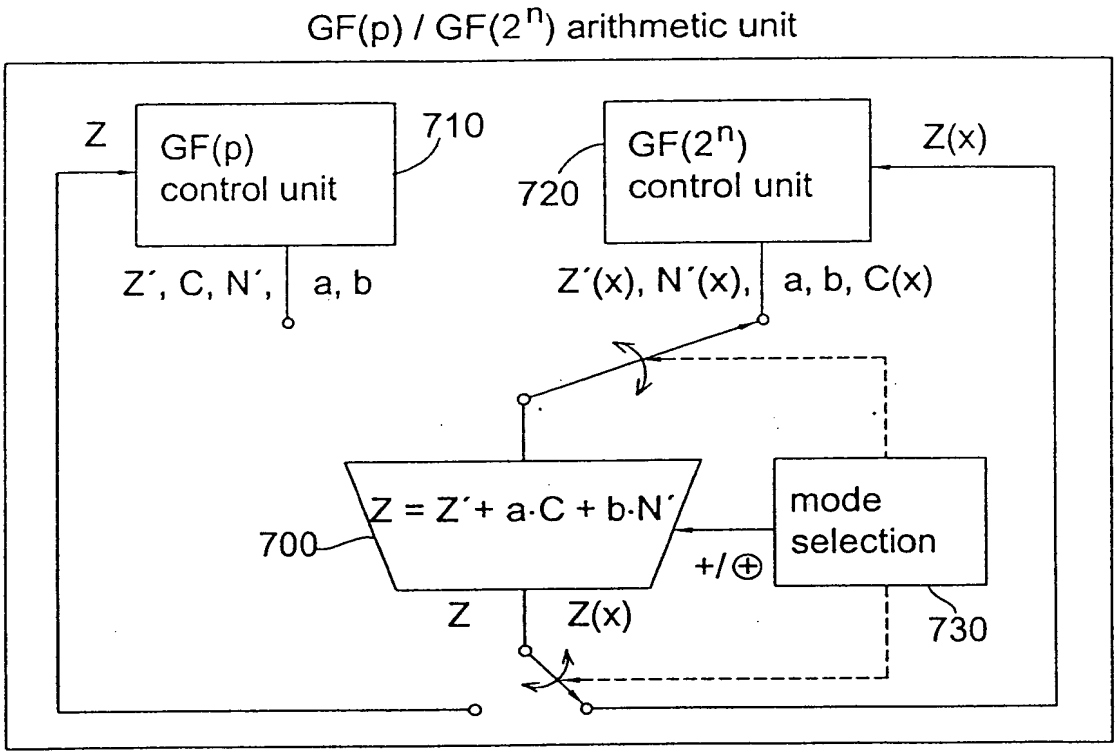

GF(p) / GF(2^n) arithmetic unit
Z
GF(p)
control unit
710
Z´, C, N´,
a, b
720
GF(2^n)
control unit
Z(x)
Z´(x), N´(x),
a, b, C(x)
Z = Z´+ a·C + b·N´
700
mode
selection
+/⊕
730
Z
Z(x)

FIG 7

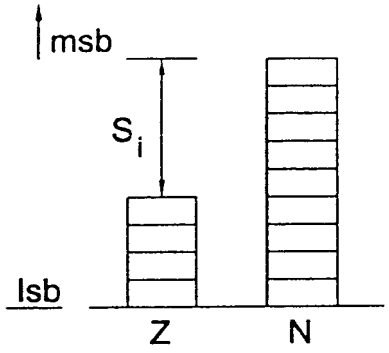


FIG 8A

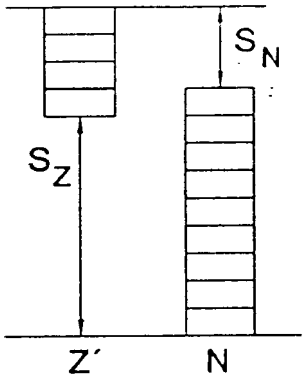


FIG 8B

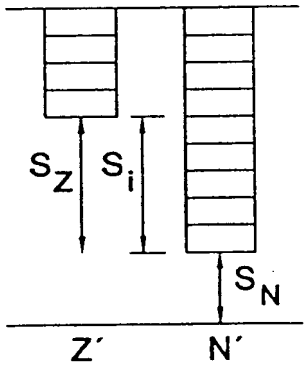


FIG 8C

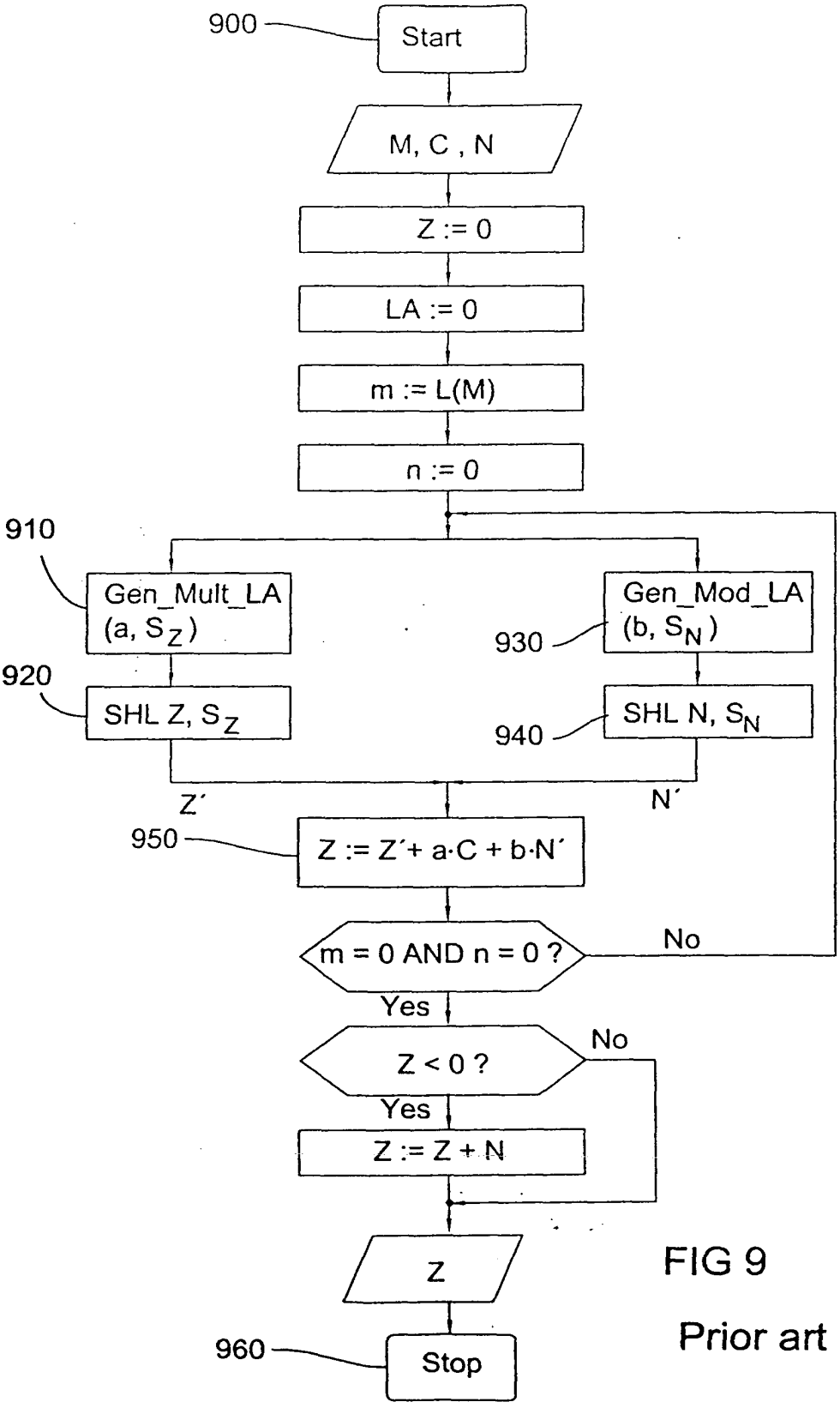


FIG 9

Prior art